JOSÉ RODRIGO FORSTER

FIREWALKING

LONDRINA - PARANÁ
2008

JOSÉ RODRIGO FORSTER

FIREWALKING

Monografia apresentada ao Curso de Especialização em Redes de Computadores e Comunicação de Dados, Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Especialista, sob orientação do Prof. Dr. João César Netto.

LONDRINA - PARANÁ
2008

Forster, José Rodrigo
Segurança em redes – firewalking / Forster. -- Londrina: UEL / Universidade Estadual de Londrina, 2008.
Orientador: Prof. Dr. João César Netto

Dissertação (Especialização) – UEL / Universidade de Londrina, 2008.
Referências bibliográficas: f. 49

1. Segurança em redes. 2. Firewall. 3. Técnicas de mapeamento de recursos - Monografia. I. Netto. II. Universidade Estadual de Londrina Especialização em Redes de Computadores e Comunicação de Dados, III. Segurança em redes - Firewalls.

JOSÉ RODRIGO FORSTER

FIREWALKING

Esta monografia foi julgada adequada para obtenção do título de Especialista, e aprovada em sua forma final pela Coordenação do Curso de Especialização em Redes de Computadores e Comunicação de Dados, do Departamento de Computação da Universidade Estadual de Londrina.

Banca Examinadora:

____
Prof. Dr. João César Netto - Orientador
Universidade Estadual de Londrina

____
Prof. Dr. Alan Salvany Felinto
Universidade Estadual de Londrina

____
Prof. Msc Fabio Sakuray
Universidade Estadual de Londrina

Londrina, Agosto de 2008.

DEDICATÓRIA

Este trabalho é dedicado primeiramente à minha esposa Viviane Mayumi Nishida, pois sem seus incentivos possivelmente não conseguiria ter concluído este trabalho, aos meus pais fonte de educação sabedoria e força para mais uma caminhada, a meus irmãos pela amizade incondicional.

Também é dedicado a meus amigos, meus colegas de trabalho, pelo incentivo para enfrentar mais uma jornada de estudos, e demais outras pessoas que contribuíram de forma positiva para a concretização deste trabalho.

AGRADECIMENTOS

Agradeço à Prefeitura do Município de Rolândia por permitir que eu me qualificasse , me auxiliando das maneiras possíveis.

Agradeço aos colegas de curso pelo apoio em busca de um mesmo ideal, e também pelas piadas e risos, que foram proporcionados nestes meses de convívio, sem os quais nosso fardo teria sido mais pesado.

Agradeço especialmente ao meu orientador pelo apoio seguro, firme e com qualidade, me dando base para a redação deste trabalho.

RESUMO

Com o crescimento da internet, a segurança das redes tornou-se um ponto fundamental de preocupação para empresas e as mais variadas instituições, pois, a informação "confiável", passou a ser o bem mais precioso. O método de controle dos fluxos de dados mais difundido é a utilização de firewalls, ou filtros de pacotes. Existem diversos arranjos de hardware e software que podem ser utilizados na elaboração de uma solução de firewall, a fim de proteger uma rede de computadores. Ao mesmo tempo existem também várias técnicas que podem ser capazes de burlar esta proteção. Neste trabalho são apresentados aspectos técnicos de alguns arranjos de firewalls conhecidos, além de técnicas para reconhecimento de sistemas operacionais de hosts alvo, serviços ativos em hosts alvo e a explicação sobre a técnica conhecida como firewalking. O estudo de caso exemplifica algumas técnicas e suas utilizações.

ABSTRACT

With the growth of the Internet, network security has become a fundamental point of concern for companies and the most varied institutions, therefore, the "reliable" information has now become the most precious. The method of control the data flow more widespread is the use of firewalls, or packet filters. There are several arrangements of hardware and software that can be used in the preparation a firewall solution to protect a computers network. At the same time there are various techniques that might be able to broke this protection. In this work are presented some technical aspects in arrangements firewalls known, as well as techniques for operating systems recognition in target hosts, services actives in target hosts and the explanation for technique known as firewalking. The case study exemplifies many of these techniques and their uses.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ACL - *Acess Control Lists*

DEC - *Digital Equipment Corporation*

DNS - *Domain Name System*

FTP - *File Transfer Protocol*

ICMP - *Internet Control Message Protocol*

IP - *Internet Protocol*

LAN - *Local Area Network*

NAT - *Network Address Translation*

POP - *Post Office Protocol*

RFC - *Request for Comments*

SMTP - *Simple Mail Transfer Protocol*

TCP - *Transmission Control Protocol*

TTL - *Time To Live*

UDP - *User Datagram Protocol*

WAN - *Wide Area Network*

WWW - *World Wide Web*

1. INTRODUÇÃO

No mundo globalizado no qual vivemos a informação torna-se a cada dia o bem mais precioso para uma empresa, governo ou qualquer outro elemento. A todo o momento nos vemos rodeados por informação que chega quase a velocidade da luz em nossos computadores. Essas informações podem variar desde textos jornalísticos, imagens geradas por satélites de bases terroristas de algum país, e que são utilizadas para servir aos interesses militares, até o fluxo de dados das contas bancárias de um usuário doméstico e seu banco. Em função da necessidade de acesso rápido à informação, a rede internet tornou-se o meio padrão de envio de informações globais, pois seus links (interligações) intercontinentais transmitem as informações em poucos segundos ao redor do planeta. Imaginando este contexto percebe-se facilmente que estas informações trafegam em um meio comum, possibilitando que pessoas mal intencionadas alterem ou desviem essas informações, pois infelizmente essa rede não é imune a ataques.

Um site de uma universidade, por exemplo, recebe milhares de visitas diariamente, mas nem todos estão interessados em estudos, existem também vários visitantes hostis que freqüentemente inundam os links destas instituições com dados maliciosos. Existe então nestas instituições e em qualquer outro tipo de instituição (empresas, órgãos públicos, etc.) que estejam conectadas à internet, a necessidade de se proteger arquivos e dados que trafegam em suas redes.

O método mais efetivo de controle do fluxo de dados que trafegam pela rede é a utilização de firewalls, ou filtros de pacotes. Firewalls são equipamentos utilizados para controlar o fluxo de dados entre redes diferentes utilizando ACL´S (Acess Control Lists), que definem quais redes, endereços e/ou portas podem passar por suas interfaces. Ou seja, os firewalls devem bloquear o tráfego indesejado e possibilitar o às funcionalidades da rede, como serviços SMTP e POP, utilizados para enviar e receber e-mails, bancos de dados, arquivos, etc. O uso mais comum dos firewalls está em isolar as redes internas das empresas da rede internet liberando o uso de determinados serviços e bloqueando serviços indesejados. Este será o foco deste trabalho.

Observando esta ótica o estudo de técnicas utilizadas por usuários maliciosos para detecção dos recursos da rede como firewalls, filtros de pacotes e roteadores, bem como o mapeamento avançado da rede, tornam-se necessários para que se consiga entender os ataques, conseguir coibi-los e garantir a segurança nas redes e a confiabilidade dos dados.

Firewalls podem ser considerados como uma abordagem de segurança, e dependendo da abordagem a ser implementada podem ser utilizados diversos tipos de serviços, arranjos de hardware e permissões de acesso que com certeza serão diferentes de empresa para empresa, pelo simples fato de que os dados, serviços e necessidades de cada uma serem diferentes. Então, é claro não existe maneira certa ou errada na hora de se configurar um Firewall.

Falar sobre técnicas de firewalking de uma maneira geral assustam por darem impressão de que são utilizadas apenas por pessoas mal intencionadas, porém estas técnicas são utilizadas por administradores de rede para verificar quão eficiente é a segurança implementada em suas redes, entender as peculiaridades sobre as diversas técnicas utilizadas por invasores, para tornar as redes cada vez mais seguras.

Este trabalho está dividido da seguinte forma: no capítulo 2 serão apresentados os conceitos sobre firewalls. No capítulo 3 serão apresentadas várias técnicas utilizadas para a obtenção de dados de redes e/ou dispositivos remotos. No capítulo 4 será abordado um estudo de caso apresentando técnicas para impedir o uso de firewalking. E finalmente no capítulo 5 serão apresentadas as conclusões e sugestões para trabalhos futuros.

2. FIREWALLS

Firewalls de acordo com [1], *É o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede*. Este dispositivo pode tanto ser um componente de software, hardware, ou um conjunto dos dois, o qual recebe normalmente o nome de Appliance.

O termo firewall é utilizado em comparação com as portas corta-fogo de edificações, que evitam o alastramento de incêndios para outros cômodos, ou seja, o firewall é utilizado para evitar que ataques se alastrem para a rede interna causando grandes transtornos.

Os firewalls devem constituir um ponto único entre a rede interna protegida e a rede internet, para que possa controlar os acessos entre essas duas redes. Os firewalls são uma forma de impor as políticas de segurança criadas pela empresa para a utilização de sua rede de computadores, pois para haver o acesso à rede externa da empresa, o firewall deve autorizar o mesmo. Sendo assim o firewall aumenta consideravelmente o nível de segurança da rede protegida e ao mesmo tempo permite acesso aos serviços da internet.
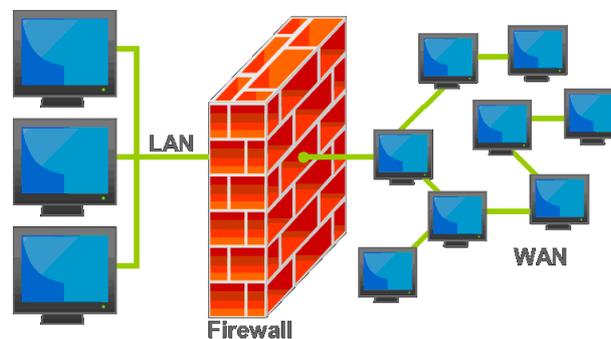
Figura 2.1 – Exemplo de separação de redes interna e internet por meio de firewall.

O controle a sistemas internos da rede pode também ser feito no firewall, impedindo acesso externo indevido a recursos internos.

Tanto os acessos internos para a internet, quanto os acessos da internet para a rede internet, obrigatoriamente devem passar pelo sistema de firewall, facilitando assim o registro de acessos. Com base nestes registros, aliados a sistemas de aviso adequados, administradores podem ser avisados sobre atividades suspeitas, como sondagens ou ataques. Estatísticas de uso de rede também podem ser visualizadas com base em registros de firewall, munindo os administradores de dados para avaliar a eficiência de links,

visualizar uso inadequado da internet pelos usuários, entre outras importantes funções para os administradores de rede.

Um projeto de políticas de firewall deve ser específico para cada rede e cada equipamento ou solução, pois cada instituição tem suas respectivas necessidades e cada equipamento suas respectivas limitações técnicas.

Geralmente existem duas políticas básicas de projetos de firewalls, uma nega todos os serviços que não são expressamente liberados e a outra permite todos os serviços que não são expressamente proibidos.

Porém a visão global das necessidades da instituição e o bom senso dos administradores é que irá definir qual das políticas será implementada e quais soluções serão utilizadas.

2.1. Evolução dos firewalls

Os firewalls começaram a surgir no final dos anos 80, como uma forma de defender as redes de computadores existentes na época, as quais estavam crescendo devido ao sucesso de redes como a ARPANET e redes militares, e a popularização da internet com o advento dos computadores pessoais. Todos estes fatores favoreciam os hackers da época que não eram atrapalhados por dispositivos de segurança, eles não eram presentes nas redes a serem atacadas.

Os firewalls surgidos em 1988 utilizavam a tecnologia de filtros de pacotes, as ACL´S, que consistem em restringir o tráfego baseando-se em endereços de IP e portas de origem e destino para permitir ou negar acesso a determinadas redes ou endereços. A filtragem é efetuada à medida que os pacotes passam pelas interfaces do equipamento de firewall. A filtragem também pode ser efetuada levando-se em consideração a interface de rede que recebeu o pacote.

O sistema de filtragem de pacotes mostra-se extremamente flexível com a utilização de filtros nos endereços IP e nas portas de serviços (TCP e UDP), pois assim pode-se bloquear portas de serviços ou endereços específicos, conhecidos como inseguros.

No sistema de filtragem de pacotes utiliza-se muito a configuração de bloquear tudo que não esteja especificamente liberado. Por exemplo, libera-se a utilização da porta 80 TCP (WWW) para as conexões iniciadas na rede interna com destino à internet e bloqueia-se todo o resto, sendo assim apenas a navegação internet está liberada e todos os

outros serviços bloqueados. Este tipo de configuração é mais trabalhoso na medida em que serviços devem ser bem estudados para não serem bloqueados por engano, porém é mais seguro, eliminando o risco de aplicações não seguras estarem liberadas sem o conhecimento dos administradores da rede. Claro que este é um exemplo básico, pois as regras de um firewall permitem filtragens muito mais complexas.

Os estudos desenvolvidos a partir dos anos 90 incluíram, além dos filtros de pacotes, os chamados filtros de estado de sessão (Stateful Firewall), que proporcionam maior flexibilidade nas configurações do firewall utilizando as tabelas de estado de conexões do protocolo TCP.

São considerados e filtrados os três estados das conexões:

- NEW – Novas conexões.
- ESTABLISHED – Conexões já estabelecidas.
- RELATED – Conexões relacionadas com outras existentes.

Os firewalls, conhecidos como "gateways de aplicação", surgiram também nos anos 90, porém nesta nova geração foi apresentado o primeiro firewall comercial, o SEAL da DEC, em 13 de Junho de 1991.

Os gateways de aplicação implementaram o conceito de "Proxy" aos firewalls. Esses necessitam um software especializado para cada tipo de serviço, ou seja, o firewall deverá receber aplicações de acordo com os serviços desejados. Ao receber as requisições de serviço dos computadores da internet, deverá gerar uma requisição ao servidor de destino, como se fosse o firewall que necessitasse do serviço, ao receber a resposta, ele a analisará antes de entregar ao solicitante do serviço. Assim os gateways "escondem" a identidade original do usuário dificultando a ação de "crackers".

Com esta solução as requisições de serviços são enviadas ao gateway de aplicação, onde, por ação do usuário ou do software especializado, é escolhido o host interno que provê o serviço. O gateway faz as verificações quanto de acordo com as regras de acesso (senhas, endereço IP, etc), e cria uma conexão com o host interno, passando a ser uma "ponte" entre os dois dispositivos, e agora passa os bytes sem fazer verificações posteriores, apenas registrando a conexão.

Como já dito, esta solução necessita software especializado para funcionar corretamente, em alguns casos pode ser necessário até mesmo um cliente modificado, o que pode ser encarado tanto como uma vantagem ou como desvantagem, pois o cliente será obrigado a ter exatamente o software necessário para se conectar ao serviço, restringindo o número de conexões. Assim conexões não seguras podem ser bloqueadas a

todos os visitantes, mas, liberadas a usuários que necessitem de conexões deste tipo, com o conhecimento e monitoração dos administradores de redes.

2.2. Exemplos de configurações de firewall

Existem vários tipos de configurações e arranjos para elaboração de projetos de firewall que vão desde a escolha de hardware, software, até o tipo de arranjo físico dos componentes. Não existe, necessariamente, um projeto ideal de firewall, pois existem várias empresas distribuidoras de softwares de segurança, que serão implementadas de acordo com as necessidades especificas de cada instituição.

A idéia central do texto a seguir é demonstrar alguns tipos mais conhecidos, mais utilizados, enfim um pequeno esboço das possibilidades existentes.

2.2.1. Firewall de filtragem de pacotes

É provavelmente o exemplo de firewall mais comum que exista, pois é o mais simples de usar em sites que não possuem muitos serviços e são, de maneira geral, pequenos e simples.

Trata-se basicamente da instalação de um roteador com filtragem de pacotes instalado no gateway de internet, com uma série de regras de filtragem de pacotes, objetivando filtrar ou bloquear protocolos e endereços.
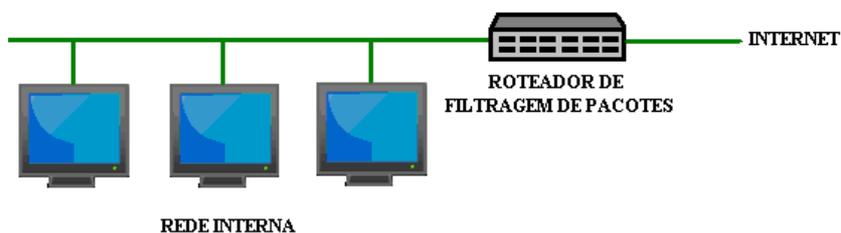
Figura 2.2 - Firewall de filtragem de pacotes

Esse tipo de firewall utiliza os esquemas da filtragem de pacotes, que como já dito possuem muita flexibilidade de configuração, podendo implementar políticas de acesso de baixo e alto nível.

Geralmente a rede interna acessa a internet diretamente, e o acesso a serviços da internet para a rede interna são bloqueados ou filtrados de acordo com as regras estabelecidas no roteador.

Existe pouca ou nenhuma ferramenta para o registro dos dados que passam pelo firewall, o que dificulta ações de monitoramento do estado do firewall pelos administradores. As regras complexas baseadas em filtragem de pacotes são difíceis de administrar e testar o que pode acabar abrindo brechas de segurança com problemas não testados.

2.2.2. Firewall Dual-Homed

Uma alternativa para a filtragem de pacotes ser melhor bem aproveitada é a utilização dos firewalls chamados firewall gateway dual-homed, um equipamento que utiliza duas interfaces de rede e sem capacidade de encaminhamento IP. Inserindo-se ainda, como proteção adicional, o roteador de filtragem de pacotes na conexão da internet, e servidores de Proxy no firewall, para oferecer acesso e serviços no mesmo.
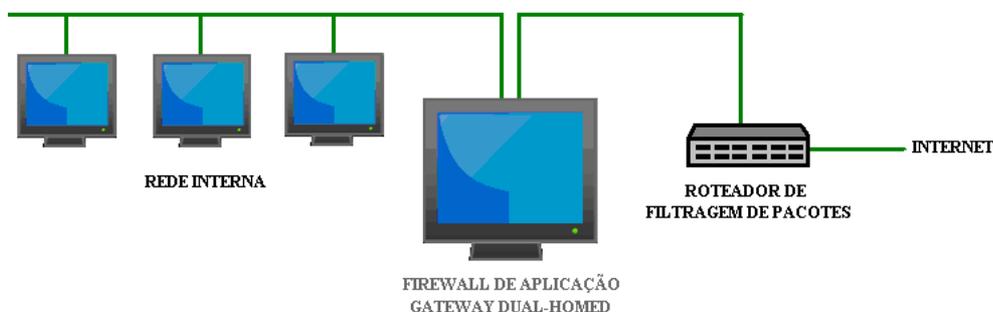
Figura 2.3 – Firewall dual-homed com roteador de filtragem de pacotes.

Este tipo de firewall implementa a configuração de negar todos os serviços que não são expressamente liberados, pois apenas os serviços com Proxies existentes são liberados, as rotas para as sub-redes são conhecidas apenas no firewall, que não passa as informações de DNS para nenhum sistema internet, expandindo significativamente a segurança.

O Proxy firewall deve implementar o uso de senhas para acesso aos sistemas da rede interna, com a utilização de softwares ou outros tipos de autenticação avançada, para que haja o registro de conexões, além dos registros normais para verificação de uso indevido, etc.

A inflexibilidade do firewall dual-homed pode tornar-se uma desvantagem para instituições que oferecem alguns serviços na internet, pois como todos os serviços são bloqueados, com exceção dos que possuem proxies outros serviços podem ser prejudicados.

2.2.3. Firewall de Sub-Rede escaneada (DMZ)

O firewall de sub-rede escaneada é uma derivação dos firewalls dual-homed, posicionando firewall e servidores de determinados serviços entre roteadores, criando assim uma sub-rede, entre a rede interna e a internet.
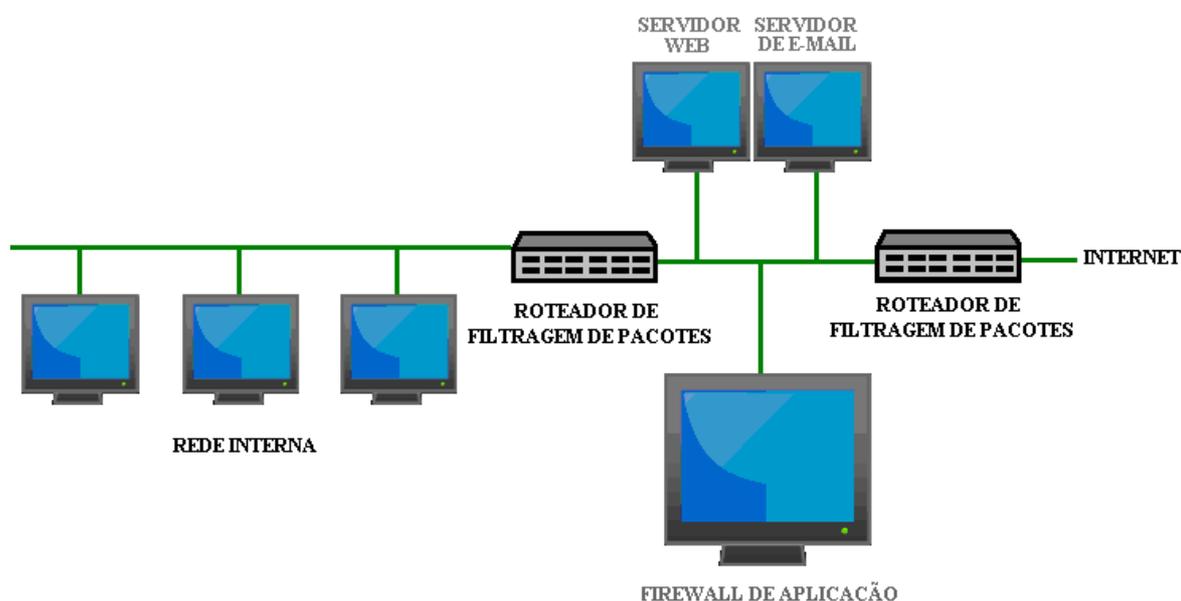
Figura 2.4 – Firewall de sub-rede escaneada

No modelo referenciado existe um roteador que fica entre a rede internet e uma sub-rede onde existe o firewall de aplicação, servidores web e de e-mail, e outro roteador entre esta mesma sub-rede e a rede interna.

O primeiro roteador pode, de acordo com as regras estabelecidas:

- Receber o tráfego de e-mail da internet e redirecionar para o servidor de e-mail.
- Receber o tráfego de e-mail do servidor de e-mail e redirecionar à internet.
- Receber tráfego de aplicações existentes no firewall de aplicação e redirecionar firewall de aplicação.
- Receber as respostas do servidor de aplicação e redirecionar à internet.
- Receber o tráfego web da internet e redirecionar para o servidor Web.

- Reencaminhar tráfego do roteador interno para a internet e devolver as respostas.
- Rejeitar todos os outros tráfegos vindo da internet.

O segundo roteador pode, de acordo com as regras estabelecidas:

- Receber o tráfego de e-mail da rede interna e redirecionar para o servidor de e-mail.
- Receber o tráfego de e-mail do servidor de e-mail e redirecionar à rede interna.
- Receber tráfego de aplicações existentes no firewall de aplicação e redirecionar firewall de aplicação.
- Receber as respostas do servidor de aplicação e redirecionar à rede interna.
- Receber o tráfego web da rede interna e redirecionar para o servidor Web.
- Encaminhar tráfego para o roteador externo para que este seja encaminhado à internet e receber as respostas.
- Rejeitar todos os outros.

O uso de dois roteadores cria redundância para dificultar a subversão dos mesmos e conseqüente acesso aos sistemas da rede interna. As configurações de acesso nos servidores na sub-rede devem ser feitas de modo a eles serem os únicos sistemas a serem conhecidos na internet, assim nenhum sistema pode ser acessado diretamente da internet e nenhum sistema acessa diretamente a internet.

Contudo os roteadores de filtros de pacotes como dito anteriormente são bastante complexos para configurar e difíceis de testar e erros de configuração podem resultar em sérios problemas de segurança.

O uso de dispositivos de segurança como os firewalls auxiliam os administradores na difícil tarefa de manter uma rede segura e operante, porém as habilidades e ferramentas utilizadas por atacantes externos à rede são muito boas.

Atacantes têm à disposição várias ferramentas, que normalmente são utilizadas por administradores para verificar a segurança e integridade de suas redes, mas, nas mãos de usuários inescrupulosos podem se tornar verdadeiras armas contra nossas redes. A grande maioria dos atacantes pode-se dizer, são jovens se aventurando na descoberta de como funcionam e como estão configuradas as redes de outras instituições e não possuem conhecimento muito profundo de como os diferentes protocolos de comunicação funcionam e não tiram total proveito das ferramentas que estão à sua disposição.

Porém existem atacantes extremamente hábeis e inteligentíssimos que tem conhecimento profundo de vários protocolos, serviços e também vasto conhecimento das vulnerabilidades dos diferentes Sistemas Operacionais e de seus vários aplicativos, ou seja, o administrador tem de ter também um vasto conhecimento, pois, a rede administrada por ele pode estar correndo perigo.

Existem várias técnicas que permitem a descoberta das características dos elementos intermediários de proteção (filtros de pacotes, firewalls, roteadores, etc.), como sistemas operacionais, serviços ativos, portas abertas, etc.. A essas técnicas damos o nome de firewalking.

3. TÉCNICAS DE FIREWALKING

Existem várias técnicas que exploram diferentes maneiras de se conhecer as vulnerabilidades de dispositivos/redes através da internet.

Essas técnicas analisam desde portas ativas em computadores até quais portas estão abertas em determinado firewall para a passagem de dados para outro computador atrás do mesmo, passando por violações do handshake, que é o estabelecimento de conexão propriamente dito entre dois computadores.

Conheceremos neste capítulo um pouco sobre várias técnicas, que foram descritas em [2].

3.1. Técnicas de inteligência utilizando ping

O primeiro passo que um atacante inteligente dará, com certeza será o reconhecimento estratégico do alvo que ele tentará invadir, pois, se ele não tiver informações suficientes, ou se o alvo tiver uma proteção alta, que tornará muito difícil a invasão ele não fará nenhum ataque a este alvo.

O reconhecimento do alvo anteriormente fará com que o atacante diminua as possibilidades de ser descoberto.

O número de escaners automatizados tem aumentado de maneira bastante rápida e como resultado o número de ataques que atingem seu objetivo, o de invadir com êxito seu alvo, tem aumentado também.

Temos então que entender os métodos que essas ferramentas utilizam, as maneiras adequadas de coibir estes ataques, as maneiras que os intrusos operam, seus objetivos com estas invasões, quais tipos de informações podem ser obtidas, nos armando de informações acerca de "assinaturas" deixadas por estes métodos. Este é o caminho para estarmos prevenidos e podermos encontrar nos logs de nossos servidores uma indicação de uma tentativa futura de obtenção de acesso aos nossos sistemas.

3.1.1. Escaneamento utilizando ICMP

Podemos utilizar pacotes ICMP ECHO REQUEST(tipo 8) para determinarmos se determinado endereço de IP alvo está ativo, pois se recebermos pacotes ECHO REPLY

(tipo 0), significa que o IP em questão está ativo, se não recebermos resposta alguma significa que o endereço encontra-se inativo.

Porém bloquear este tipo de escaneamento é bastante fácil, basta bloquear pacotes ICMP vindos de fora de nossa rede.

3.1.2. Broadcast ICMP

O envio de pedidos ICMP ECHO à rede ou aos endereços de broadcast produzirá todas as informações para um mapeamento completo da rede alvo de uma forma simplificada, pois o pedido é enviado a todos os hosts da rede, que responderam ao endereço IP do atacante, após um ou dois pacotes terem sido enviados. Isso se as maquinas forem baseadas em UNIX, pois máquinas Windows irão ignorá-los.

3.1.3. ICMP – Não ECHO

Porém o bloqueio de pedidos ICMP ECHO não é suficiente, pois existem os protocolos ICMP não ECHO, como o TIMESTAMP (ICMP tipo 13), que permitem a um sistema consultar outro, e o ADRESS MASK REQUEST (ICMP tipo 17), que é destinado a máquinas com boot pela rede e que obtém a máscara de rede no período do boot.

Ao utilizar ferramentas como icmppush e icmpquery podemos realizar esse tipo de scan para verificarmos quais dispositivos estão ativos.

3.1.4. Escaneamento utilizando TCP

Handshake é o nome dado ao processo de estabelecimento de conexões TCP e é a combinação de três segmentos de dados, trocados entre os computadores.

- O 1º deles é o envio por parte de uma máquina cliente, de um segmento de dados SYN que especifica o número de porta do servidor ao qual o cliente quer se conectar, juntamente com um número de seqüência inicial do cliente.
- Se o servidor não possui o serviço requerido na porta especificada o processo é interrompido por um RESET, se o serviço estiver ativo é dado o 2º passo, quando o servidor responde com um conjunto de dados SYN, juntamente com

a seqüência inicial do servidor. Então o servidor reconhecerá o SYN do cliente e enviará um conjunto de dados aceitando a conexão que se trata de um ACK do cliente SYN+1.

- O cliente reconhece o SYN do servidor pelo conjunto de dados SYN+1.
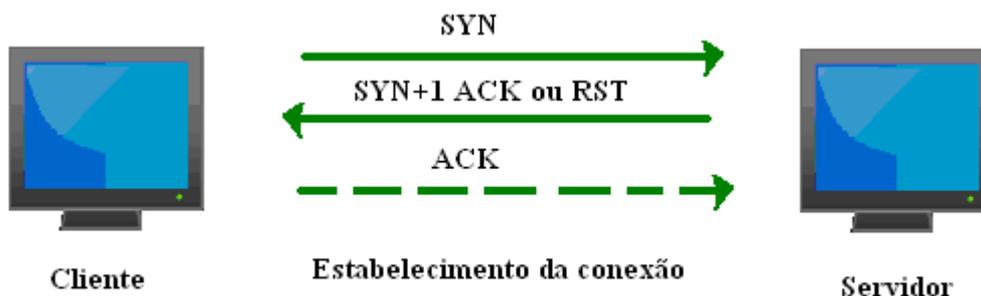
Figura 3.1 - Handshake na conexão TCP

Nesta técnica ao invés de enviarmos pacotes ICMP ECHO, enviamos pacotes TCP ACK para a rede alvo, os números de portas vão depender de que serviço queremos verificar o status. Por exemplo, podemos usar a porta 80 (www). Se recebermos alguma resposta teremos certeza de que há alguma coisa ativa no endereço alvo.

3.1.5. Escaneamento utilizando UDP

Este método se baseia nas mensagens ICMP de porta inacessível, iniciadas por uma porta UDP fechada. Se após um envio de um datagrama UDP para uma porta UDP do sistema alvo, não recebermos nenhuma mensagem ICMP de porta inacessível, consideramos tal porta como aberta.

Porém muitos serviços UDP não respondem corretamente quando solicitados, e pacotes UDP podem ser “dropados” por roteadores e por firewalls configurados com esta diretiva, tornado este tipo de escaneamento não confiável.

3.2. Port scannings

As técnicas anteriores identificam quais sistemas estão ativos, agora iremos conhecer algumas técnicas que nos auxiliam na descoberta de quais serviços estão realmente em execução, ou então em um estado conhecido como “escutando” nas portas

UDP e TCP. Este tipo de escaneamento ajuda na identificação do sistema operacional e da aplicação em uso.

3.2.1. Escaneamento de conexão TCP

Com este tipo de varredura usamos o mecanismo básico de estabelecimento de conexão TCP. Para abrir uma conexão a uma porta de nosso interesse na máquina alvo:

1. Um pacote SYN é enviado para a porta de nosso interesse na máquina alvo.
2. Agora é esperar para ver qual o tipo de pacote é enviado de volta a partir do alvo.
   • Se um pacote SYN / ACK é recebido, normalmente significa que a porta está em um estado ESCUTAR.
   • Se um pacote RST / ACK é recebido, normalmente significa que a porta não está a ouvir e a ligação será RESETADA.
3. Se o pacote SYN / ACK foi recebido nós terminamos o handshake em três vias enviando um ACK.
4. A conexão é encerrada após o estabelecimento completo do processo de conexão ter sido concluído.

Este tipo de pesquisa é facilmente detectado. Pois cada uma dessas conexões é gravada no log da máquina gerando uma série de conexões e mensagens de erro imediatamente após cada uma delas ser iniciada.

3.2.2. TCP SYN Scan

Este tipo de varredura é bastante parecido com o escaneamento da conexão TCP, porém difere-se desta por não abrir uma conexão completa.

Nesse escaneamento envia-se um pacote SYN no início do handshake e aguarda-se a resposta, se obtivermos um pacote RESET significa que a porta não está escutando. Se recebermos um pacote ACK indica que a porta está escutando e então enceramos a conexão enviando um pacote RESET. Este procedimento pode impedir gravações nos logs dos servidores, pois alguns deles não geram logs de conexões que não forem completamente estabelecidas.

3.2.3. Técnicas de escaneamento invisível

O termo “Invisibilidade” segundo [2] pode também ser entendido como uma família de técnicas de varredura, que passem por mecanismos de filtragem, não sejam

identificados por mecanismos de logging do sistema alvo, e que tentam esconder-se no tráfego atual da rede ou site alvos.

Esta família de técnicas foi dividida em duas partes. Invisibilidade explícita, onde o atacante envia variados tipos de pacotes diretamente ao sistema alvo de uma maneira que ele se torna "invisível" e mapeamento Inverso que não faz o escaneamento diretamente ao sistema alvo.

Os tipos de ataque que são ligados à invisibilidade explícita são:

- Escaneamento SYN/ACK: Nesse tipo de escaneamento é enviado um pacote SYN/ACK que é a segunda parte do handshake. O TCP entende que este pacote é um erro. No caso de a porta estar fechada o TCP responde com um RESET e se a porta estiver aberta nenhuma resposta é enviada. Assim sabemos se a porta em questão encontra-se fechada;
- Utilizando pacotes FIN;
- Escaneamento XMAS TREE: que envia pacotes TCP para todas as portas do host alvo, com todas as flags TCP definidas (URG (urgent), PSH (push) e FIN (finish)), onde se verificam as portas escutando. Se a porta no host alvo estiver fechada, o comum o host atacante receber um pacote TCP Reset, no caso de a porta estar aberta, nenhuma resposta é recebida.
- NULL SCAN: Envia pacotes TCP com todas as flags desligadas, onde os sistemas deveriam enviar de volta um RESET para todas as postas fechadas ;

Os tipos de ataque que são ligados ao mapeamento inverso são:

- RESET Scan: Os roteadores gravam uma lista de endereços de Host/rede inacessível e mensagens de tempo excedido que recebem, neste tipo de escaneamento o roteador é sondado para obter uma lista destes IP´s. gerando assim uma possível lista de hosts/redes ativas.
- Domain Query answers: Neste tipo de escaneamento são enviadas ao domínio respostas à requisições nunca solicitadas, para se obter mensagens ICMP inacessível de hosts ou sub-redes que não existem.

3.3. Varredura de PROXY FTP

Uma varredura das portas TCP pode ser iniciada através de um servidor FTP com o recurso de proxy ativado. Pode ser gerada uma conexão à este servidor que tenha permissões de gravação global, estando atrás de um firewall, e em seguida escanear as portas que este firewall bloqueia.

Se o atacante tiver permissões de gravação totais no diretório do FTP, provavelmente terá também permissões para as portas que você encontrará abertas. Utilizando este tipo de ataque podemos verificar todas as portas do alvo através do envio de comandos seqüenciais para todas as portas esta pesquisa é bastante lenta, porém eficiente, se o recurso de proxy estiver ativo. Hoje muitos servidores FTP têm este recurso desativado, porém existem muitos servidores onde este recurso continua ativo.

3.4. Técnicas de PORT Scanning

3.4.1. "Port scan" randômico

Existem sistemas de detecção de intrusão que normalmente estão procurando tentativas de conexões seqüenciais, como um escaneamento com o número crescente de portas (primeiro se faz um escaneamento na porta 21, depois na porta 22, então na porta 23, etc.).

Randomizar a seqüência de portas pode evitar detecções.

3.4.2. Escaneamento lento

Sistemas de detecção de intrusão possuem o "tempo de resposta de detecção", que é o período de tempo durante o qual é analisado todo o tráfego de rede, para a verificação e possível detecção de um "port scan".

Se o atacante puder determinar qual é, aproximadamente, esse período de tempo pode reduzir a probabilidade de ser detectado, ou até mesmo não ser detectado pelo sistema de detecção de intrusão, por isso escaneamento lento, pois pode levar até mesmo dias para esse tempo terminar.

3.4.3. Fragmentação

Todos os pacotes IP que contenham dados podem ser fragmentados, normalmente temos como padrão enviar no primeiro pacote a porta de destino, porta de origem juntamente com os campos de flags IP.

O tamanho mínimo de um pacote TCP, definido na RFC 791, é de oito octetos de dados que é suficiente para os números de porta de origem e destino, forçando o campo flags a ir no segundo segmento de dados. Esta manobra pode fazer com que firewalls entendam incorretamente porções do scan, como se fossem apenas fragmentos de tráfego que já passaram pelas ACLs.

3.4.4. Falsificação

Alguns scanners incluem opções de chamariz ou falsificação de endereços nos ataques, onde o atacante disfarça seu host como sendo um host da rede atacada, escaneando seu próprio host também. Assim torna-se difícil a tarefa de determinar qual o host atacante.

A detecção de quais hosts são os chamarizes, pode ser feita analisando os valores do campo TTL (Time To Live) dos pacotes escaneados, se eles têm o mesmo valor provavelmente foram enviados do mesmo host.

Outra forma de detecção do verdadeiro host atacante é tentar encontrar o IP fonte do traceroute, pois se houver IP´s não roteáveis, ou IP pertencente a um host que não está ativo, pode significar que encontramos nosso atacante.

3.4.5. Ataques coordenados

Testar alguns host alvo através de um único IP atacante dentro de um determinado período de tempo normalmente irá ligar o alarme dos sistemas de detecção de intrusão.

Quando um grupo de atacantes está trabalhando em conjunto para alcançar um objetivo comum, que é tentar obter acesso não autorizado a uma rede alvo, dá-se o nome de ataques coordenados. Se vários IPs escanearem uma rede alvo, cada um deles escaneia um determinado serviço em uma máquina em um determinado período de tempo diferente e, por isso, seria quase impossível de se detectar estes scans.

Ataques coordenados podem ser utilizados para atacar um único host ou até mesmo uma rede inteira. Quando os esforços de ataque coordenados são destinados a um determinado host, a detecção depende do período de tempo que estes escaneamentos levam.

Ataques coordenados, quando lançados com inteligência, são a forma mais discreta de sondar um alvo. A maior parte destes ataques ainda não é detectada.

3.5. Detecção de sistema operacional

Atualmente a maioria dos casos de falha de segurança são dependentes do sistema operacional instalado no host a ser escaneado, por este fato, é importante que o atacante descubra previamente qual o sistema operacional de seu alvo, para elencar possíveis vulnerabilidades. Algumas das técnicas de detecção do sistema operacional serão mostradas abaixo.

3.5.1. Banners de serviços

Alguns tipos de serviços podem vazar informações sobre o tipo de sistema operacional onde estão instalados, fazendo com que com um simples acesso ao serviço mesmo que sem a conexão completa o atacante consegue verificar qual o sistema operacional do host.

Um exemplo clássico é o serviço de TELNET que em sua saudação, já identifica qual o sistema operacional.

3.5.2. Registro Hinfo do DNS

Um par de strings sobre determinado host pode ser usado no registro de informações do servidor DNS para identificar o hardware e o sistema operacional deste host, como no exemplo abaixo:

www IN HINFO "Sparc Ultra 5" "Solaris 2.6".

Esta técnica raramente é eficaz porque os administradores evitam utilizar este registro, por sua vulnerabilidade.

3.5.3. TCP/IP Stack Fingerprinting

Stack Fingerprinting é uma técnica que utiliza as variações na implementação da pilha TCP para determinar o tipo do sistema operacional remoto.

A idéia é a de enviar pacotes TCP específicos para o IP alvo e observar a resposta. Determinados grupos ou sistemas operacionais irão enviar resposta que será exclusiva. A resposta varia porque os diferentes sistemas operacionais implementam suas próprias pilhas IP. Isso ocorre devido às diferentes interpretações de orientações de RFC específicas quando desenvolvedores escreveram sua pilha TCP / IP

3.5.4. Sonda FIN

Segundo a RFC 793 ao se enviar um pacote com a flag FIN setada (sem mais dados da origem a serem enviados) para uma porta aberta, o procedimento correto é não responder este pacote, porém implementações de pilha Windows, CISCO, entre outras irão responder com um RESET.

3.5.5. Pacote SYN com flag indefinida

Ao se enviar um pacote SYN para os host alvo com a flag indefinida, alguns sistemas operacionais irão resetar esta conexão.

Hosts com Sistema operacional LINUX com a versão do Kernel anterior a 2.0.35 irão manter a flag setada nas respostas.

3.5.6. Número de seqüência inicial TCP

As solicitações de conexões TCP também podem dar ao atacante informações sobre o sistema operacional no host alvo.

Ao localizar padrões dos números de seqüência inicial escolhida pelas implementações TCP no ato de responder à solicitação de uma conexão, podemos dividir as respostas em quatro grupos:

- Tradicional 64k (UNIXs mais antigos);

• Incrementação Randômica (FreeBSD, DG-UX, IRIX, novas versões do Solaris);
• Verdadeira numeração “aleatória” (Linux);
• Tempo dependente dos módulos (MS Windows);

3.5.7. Fragmentação de bits

Alguns sistemas operacionais definem a Não fragmentação de bits para melhorar a performance.

Esse comportamento pode dar ao atacante mais informações sobre o sistema operacional do alvo.

3.5.8. Janela inicial TCP

Algumas implementações de pilha de têm um tamanho único na janela inicial de seus pacotes devolvidos. AIX, por exemplo, é o único sistema operacional usando o valor 0x3F25. OpenBSD e FreeBSD usam 0x402E.

3.5.9. Valor ACK

Em alguns casos pilhas IP podem diferir no valor que eles usam para o campo ACK. Por exemplo, enviando um pacote FIN, PSH, URG a uma porta fechada. A maioria das implementações irá definir acknowledgement no pacote a ser devolvido com o mesmo número de seqüência recebido. O Windows responde com um campo ACK que é o número de seqüência +1.

3.5.10. Mensagem de erro ICMP

Apenas alguns sistemas operacionais seguem a RFC 1812, que limita a taxa de envio de mensagens de erro, que podem ser baseadas em um contador de quantos pacotes foram dropados de um host origem, baseadas em um timer enviando uma mensagem de erro ao host de origem ou no máximo uma mensagem a cada determinado período de tempo ou ainda baseado na largura de banda da rede limitando a velocidade do pacote à uma fração da largura de banda disponível

Um atacante pode usar esse recurso para enviar pacotes UDP ao acaso, com a porta UDP alta e contar o número de mensagens inaccessíveis recebidas dentro de um determinado período de tempo.

3.5.11. Citações em mensagens ICMP

Mensagens de erro ICMP devem citar uma pequena quantidade de informações a partir da mensagem ICMP que causou o erro, para demonstrar o que causou o erro.

A informação citada, por quase todas as implementações, quando a mensagem de porta inacessível é recebida, é o cabeçalho IP+8 bytes. Solaris envia mais informações do que é necessária e o Linux envia mais informações ainda.

3.5.12. Integridade de mensagens de erro ICMP ECHO

Ao enviar de volta uma mensagem de erro ICMP, algumas implementações de pilha podem alterar o cabeçalho IP de maneira muita particular.

Se um atacante examina os tipos de alteração que tem sido feito nos cabeçalhos, ele será capaz de fazer algumas suposições sobre o sistema operacional do alvo.

3.5.13. Tipos de Serviços

Quando uma mensagem de PORTA ICMP inacessível é enviada, um invasor pode examinar o campo tipo do serviço, pois, várias implementações usam o valor 0 para este campo, o Linux, por sua vez, utiliza 0xC0.

3.5.14. Implementação da fragmentação

A sobreposição de fragmentos de pacotes é efetuada das mais diferentes maneiras de acordo com a implementação de pilha, conseqüentemente de acordo com cada sistema operacional específico.

Pois algumas destas implementações substituem porções antigas de dados por dados recentes ou vice-versa, quando os dados são reagrupados.

3.5.15. Opções TCP

Existem duas RFC´s que definem as opções TCP, a RFC 793 que define as opções TCP e a RFC 1323 define as opções TCP mais avançadas. Então devemos levar em consideração que:

• Nem todos os hosts implementam opções TCP

• Ao enviar uma consulta com um conjunto de opções para o host alvo, o host alvo irá configurar a opção na resposta apenas se suporta-la.

• Nós podemos testar todas as opções, ao mesmo tempo, se nos enviarmos um pacote que inclua todas as opções.

Ao se analisar o pacote de resposta, você verá no campo Opções quais opções foram definidas. Estas são as opções suportadas. Alguns sistemas operacionais suportam muito poucas suportam opções avançadas e outros suportam todas.

3.6. Traceroute ou Expiração IP

É uma técnica de mapeamento de rede, utilizada para mapear dispositivos de encaminhamento (roteadores), mostrando todos os dispositivos até o host de destino, opera na camada IP, utilizando pacotes TCP, UDP ou ICMP.

Este tipo de escaneamento utiliza o campo TTL do pacote IP, que limita a vida útil de quaisquer de pacotes na internet. Ao ser enviado o pacote possui um valor de campo TTL, quando o pacote está no roteador e será repassado ao próximo roteador no caminho até o host destino, este valor é diminuído. Se esta redução apresentar um valor igual a zero ou menos, o roteador irá enviar de volta ao host que enviou o pacote uma mensagem de erro ICMP TTL expirado em trânsito, juntamente com seu endereço, permitindo que o host original saiba em qual roteador o pacote expirou.

O traceroute inicia a transmissão dos pacotes com o campo TTL igual a 1 e aumenta o valor a cada rodada (TTL = TTL+1), que por padrão cada rodada constitui-se de três pacotes, podendo então enumerar os roteadores entres os dois hosts. Se o escaneamento é feito utilizando pacotes UDP, a porta de destino é incrementada a cada pacote enviado. Quando o pacote chega a seu destino, o host final envia um pacote ao host que originou o escaneamento, encerrando o mesmo.
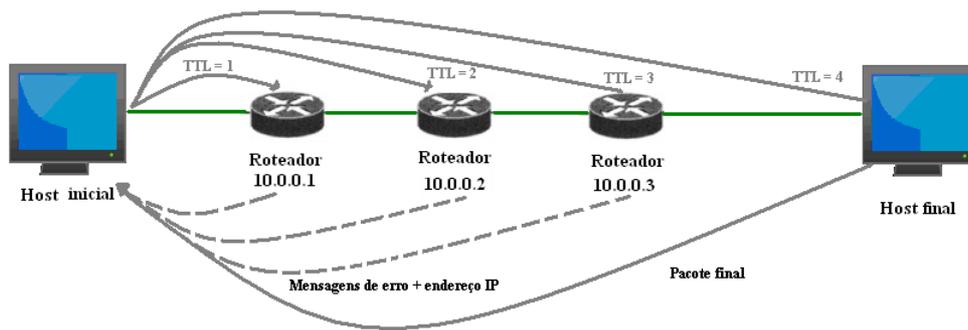
Figura 3.2 - Traceroute

3.6.1. Subterfúgio de protocolo

Ao fazermos um traceroute para um host atrás de um firewall, quando a sondagem atingir o firewall, um filtro ACL pode descartar nosso pacote. Porém o traceroute, como dito anteriormente pode trabalhar com qualquer protocolo de transporte.

No caso de haver um firewall bloqueando todo o tráfego de ingresso à uma rede, exceto pedidos e respostas ICMP, traceroute pode enviar pacotes ICMP para verificar hosts atrás deste firewall.

3.6.2. Seeding de porta inicial

Em um cenário mais comum de rede protegida por firewall todo o tráfego de ingresso é proibido exceto a porta UDP 53 de consulta DNS.

Se o atacante possui esta informação, além do número de hops até o firewall destino, e que a cada rodada são enviados três pacotes, ele pode determinar qual será o número de porta que chegará ao firewall. Para enganá-lo, fazendo nossos pacotes se passarem por consultas DNS, utilizando um cálculo matemático para saber qual o número de porta ele irá colocar em seu pacote inicial de sondagem.

(porta_alvo - (n de hops * pacotes por rodada)) - 1

Por exemplo, se utilizarmos o número de hops da Figura 3.2 teremos o seguinte cálculo:

$$(53 - (4 * 3)) - 1 = 40$$

Ou seja, nosso escaneamento traceroute terá como porta inicial a 28 e após todas as rodadas chegará ao destino com o valor de porta igual a 53, sendo bem sucedida em sua chegada ao firewall, pois se faz passar por um pacote de consulta DNS.

3.7. Firewalking

A técnica conhecida como firewalking é uma junção do traceroute com os port scans, pois, utiliza elementos destas técnicas para alcançar seus objetivos – criar um mapa apurado da topologia da rede atrás do firewall e determinar o conjunto de regras ACL do firewall ou filtro de pacotes. Porém, várias das técnicas vistas até agora podem ser consideradas como complementos para o firewalk tornando muito mais rigoroso o mapeamento avançado desta rede.

Para a utilização do firewalking é necessário que se conheça de antemão o endereço do último gateway (firewall) no caminho até a rede a ser escaneada e o endereço de um host atrás do firewall.

O Primeiro IP serve para orientar o escaneamento, pois se algum pacote enviado não devolver uma resposta podemos assumir que tal tipo de pacote é bloqueado e o segundo IP serve como métrica para o fluxo dos dados do escaneamento.

Utilizando esta técnica podemos usar vários tipos de ataques para recolher informações. Se o gateway permite o tráfego, ao repassar os pacotes ao host alvo os mesmos irão expirar e serão devolvidos em uma mensagem de erro ICMP TTL excedido em trânsito, se não permitir tal tráfego os pacotes serão descartados, onde nosso host original não receberá resposta alguma. Este tipo de sondagem enviada de forma sucessiva a diversas portas, com protocolos diferenciados, guardando quais deles receberam respostas, irá definir uma versão apurada da ACL no firewall.
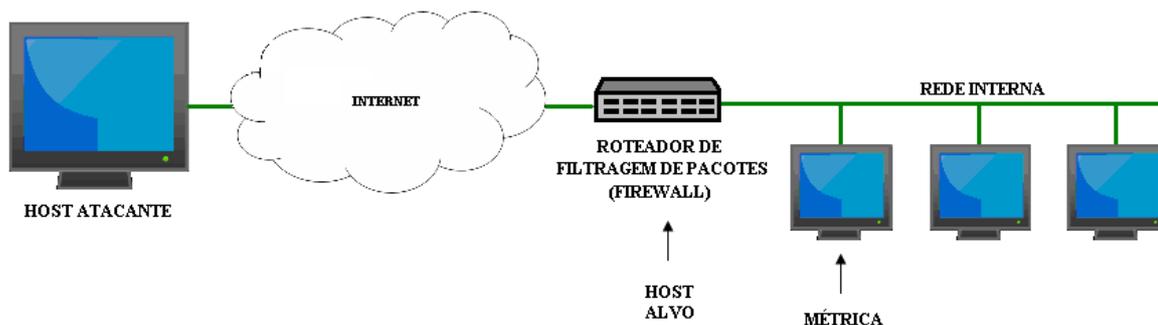
Figura 3.3 - Firewalking

Em uma primeira fase de descoberta da rede, pois não sabemos a distância em hops do nosso alvo, conhecida como ramping, se obtém o TTL IP correto até o host alvo, como em um traceroute, enviando pacotes com sucessivos incrementos do campo TTL para descobrir a quantidade de hops até o host alvo.

Ao sabermos qual a contagem de hops até o nosso gateway alvo, poderemos avançar para a próxima fase, o escaneamento.

O escaneamento é simples, o firewalk envia uma série de pacotes TCP e UDP ao host definido como métrica e dispara um "timer" que define um "timeout". Se este tipo de pacote for aceito pela ACL do host alvo, o host atacante recebe uma mensagem ICMP TTL expirado em trânsito e a porta é considerada aberta. Se o host atacante não receber nenhuma resposta antes do tempo do timer expirar, assume–se que o pacote violou a ACL e foi descartado e a porta é considerada fechada.

Porém se o host métrica for topologicamente junto ao gateway alvo, ou seja, se o host métrica for exatamente um hop do gateway alvo e o pacote passar pela ACL, significa que o pacote chegou ao seu destino final e será processado no host métrica. Então a resposta ao host atacante irá depender do tipo de pacote enviado no escaneamento. Será possível agora ao host atacante fazer um port scan no host métrica, através do gateway alvo, embora de forma limitada, fazendo uma varredura nas aplicações ativas.

3.7.1. Caminhada lenta

Pacotes IP podem ser descartados por uma série de razões, se esse descarte não for causado por filtros proibitivos com certeza será por perda de dados, que podem ocorrer por uma rede congestionada. Em um escaneamento do tipo firewalk as perdas devem ser mantidas a um nível absolutamente mínimo, portanto devem-se controlar as perdas para melhorar a capacidade de escaneamento.

O melhor que pode-se fazer na maioria dos casos, a melhor prática é a redundância do número de sondagens que enviamos. A menos que haja algum grave congestionamento de rede devemos obter respostas através das sondagens. Porém pode ser que estas sondagens sejam descartadas por outros dispositivos de filtragem de pacotes existentes no caminho entre o host atacante e o gateway alvo, ou seja, o host atacante não irá receber nenhuma resposta e considerará a porta como fechada, gerando assim falsos negativos para pacotes que estejam sendo descartados. Esta não é uma perda estranha, o

simples fato de se enviar mais pacotes de dados não irá fazer diferença alguma, pois o filtro intermediário é que está descartando os pacotes..
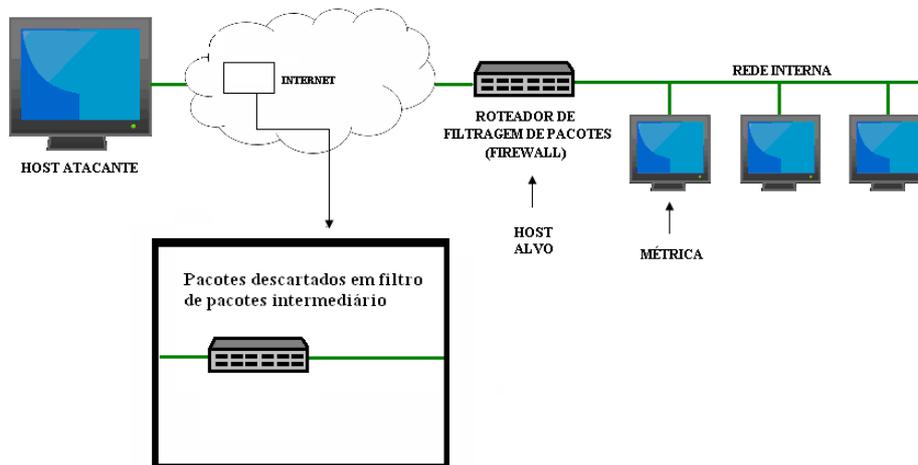
Figura 3.4 – Descarte de pacotes gerado por filtro de pacotes intermediário

Nestes casos devem ser realizadas “caminhadas lentas”, que são parecidos com exames normais, no entanto, neste caso todos os hops na rota até o host alvo devem ser escaneados, executando uma fase de ramping em cada um dos hops intermediário antes do escaneamento.

Isto impedirá falsos negativos devido ao bloqueio em filtros intermediários e dará mais confiabilidade aos relatórios do firewalk, agora podemos determinar que as portas identificadas como bloqueadas no host alvo não são falsos negativos.

Se existirem muitas portas sendo bloqueadas por filtros intermediários, as quais forem necessárias ao escaneamento do host alvo, uma solução simples pode ser o deslocamento físico do host atacante, para tentar não ofender a rota pelo filtro intermediário.

4. UTILIZANDO TÉCNICAS DE FIREWALKING

Neste capítulo abordaremos a utilização de algumas das técnicas de firewalking de uma maneira mais prática, formulando estudos de caso para alguns dos ataques citados anteriormente. O objetivo é testar sistemas operacionais em uma rede comum, verificando como os ataques funcionam. Utilizaremos nestes ataques simulados, o programa NMAP para Windows e a suite de segurança Backtrack 3, uma distribuição live CD baseada no Linux Slackware. Verificaremos servidores e estações de trabalho a procura de falhas de segurança e serviços que poderiam estar desativados, sem prejuízo ao funcionamento da rede e objetivando maior segurança da informação.

Nmap é um utilitário de segurança, desenvolvido pelo autodenominado “hacker” Fyodor, é utilizado para a descoberta de computadores e serviços ativos em uma rede. Suporta port scannings, descoberta de hosts, detecção de versão de serviços ativos e descoberta de Sistema operacional. Utilizaremos neste trabalho a versão gráfica do Nmap por haver uma intuitividade em seus comandos, pelo uso do gerador de comandos.

O Backtrack 3 é uma distribuição linux baseado no Slackware, possui vários programas para recolhimento de informações, port scanners e o programa firewalk inclusos, o que o torna uma ferramenta muito importante para consultores de segurança que visitam clientes e muitas vezes precisam fazer uma varredura para identificar possíveis problemas, sem precisar baixar e/ou instalar programas de verificação de segurança.

As ferramentas são gratuitas e estão disponíveis na internet, nos seguintes endereços eletrônicos:

- Bactrack 3 - http://www.remote-exploit.org/backtrack_download.html
- NMAP - http://nmap.org/download.html

Por razões óbvias não utilizaremos neste estudo de caso os endereços reais dos hosts testados, em seus lugares utilizaremos endereços privados definidos na RFC 1918.

As pesquisas realizadas sobre hosts alvo neste trabalho serão bastante simples, apenas para interesse didático, porém as ferramentas utilizadas podem prover escaneamentos bastante complexos, irá depender do nível de aprofundamento teórico de quem estiver utilizando os mesmos.

4.1. Utilizando o NMAP

Não abordaremos neste trabalho a instalação do Nmap, pois a mesma não se mostra relevante utilizaremos somente seu ótimo port scan, e algumas de suas outras funcionalidades para exemplificarmos alguns dos conceitos mostrados anteriorente.

4.1.1. Escaneamento utilizando TCP

Executamos o ataque utilizando a conexão TCP, em um Servidor Windows 2000 Server. A sintaxe do ataque foi a seguinte:

nmap -sT 192.168.1.1

E tivemos o seguinte resultado:

Starting Nmap 4.68 (http://nmap.org) at 2008-08-22 10:15 Hora oficial do Brasil

//Lista-se quais as portas consideradas "interessantes" e quais os serviços presentes nas mesmas.

Interesting ports on 10.1.249.1:

Not shown: 1694 filtered ports

PORT STATE SERVICE

7/tcp open echo

9/tcp open discard

17/tcp open qotd

21/tcp open ftp

25/tcp open smtp

53/tcp open domain

88/tcp open kerberos-sec

110/tcp open pop3

119/tcp open nntp

139/tcp open netbios-ssn

143/tcp open imap

389/tcp open ldap

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

1026/tcp open LSA-or-nterm

1029/tcp open ms-lsa

1050/tcp open java-or-OTGfileshare

1068/tcp open instl_bootc

3268/tcp open globalcatLDAP

3389/tcp open ms-term-serv

MAC Address: 00:30:4F:37:9A:C5 (Planet Technology) → **Mac address da placa de rede e fabricante da mesma**

Read data files from: C:\Arquivos de programas\Nmap

Nmap done: 1 IP address (1 host up) scanned in 340.219 seconds

Raw packets sent: 1 (42B) | Rcvd: 1 (42B)

Verificamos que o NMAP nos mostra quais os números das portas, o protocolo de comunicação, o status da porta (open, filtred) e qual serviço está ativo na porta. Estas informações podem ser muito úteis a um atacante.

Após este teste foi implementado antes deste host um firewall, com o IPtables, devidamente configurado para que nenhum acesso externo à este computador fosse permitido entrar na rede a não ser o Serviço de FTP, além de implementarmos o Serviço de NAT e Stateful firewall ao mesmo e novamente fizemos o mesmo escaneamento. Recebemos então a seguinte resposta:

Starting Nmap 4.65 (http://nmap.org) at 2008-08-25 18:17 Hora oficial do Brasil

Note: Host seems down. If it is really up, but blocking our ping probes, try -PN

Nmap done: 1 IP address (0 hosts up) scanned in 3.547 seconds

O Nmap sequer conseguiu identificar se o host estava ativo, então seguimos a instrução que o NMAP nos passou e tentamos o seguinte comando:

nmap -sT -PN 192.168.1.1

Starting Nmap 4.65 (http://nmap.org) at 2008-08-25 18:25 Hora oficial do Brasil

Interesting ports on 192.168.1.1 (192.168.1.1):

Not shown: 1714 filtered ports

PORT   STATE SERVICE

21/tcp open ftp

Nmap done: 1 IP address (1 host up) scanned in 122.984 seconds

Como podemos observar apenas a porta de nosso interesse é exibida, dificultando em muito o trabalho de um possível atacante.

4.1.2. Escaneamento usando o SYN Scan

Executamos agora o ataque utilizando a conexão um SYN Scan, em um Servidor Linux Conectiva 10. A sintaxe do ataque foi a seguinte:

nmap -T Aggressive -A -v 192.168.1.2

E tivemos o seguinte resultado:

Starting Nmap 4.65 (http://nmap.org) at 2008-08-25 17:51 Hora oficial do Brasil

Initiating Ping Scan at 17:51

Scanning 192.168.1.2 [2 ports]

Completed Ping Scan at 17:51, 0.36s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 17:51

Completed Parallel DNS resolution of 1 host. at 17:51, 0.09s elapsed

Initiating SYN Stealth Scan at 17:51

Scanning 192.168.1.2.track.net.br (192.168.1.2) [1715 ports]

Increasing send delay for 192.168.1.2 from 0 to 5 due to 15 out of 37 dropped probes since last increase.

Discovered open port 8009/tcp on 192.168.1.2

Discovered open port 111/tcp on 192.168.1.2

Discovered open port 8080/tcp on 192.168.1.2

Completed SYN Stealth Scan at 17:52, 35.61s elapsed (1715 total ports)

Initiating Service scan at 17:52

Scanning 3 services on 192.168.1.2.track.net.br (192.168.1.2)

Completed Service scan at 17:53, 44.81s elapsed (3 services on 1 host)

Initiating OS detection (try #1) against 192.168.1.2.track.net.br (192.168.1.2)

Retrying OS detection (try #2) against 192.168.1.2.track.net.br (192.168.1.2)

//Verifica a quantidade hops até o host alvo

Initiating Traceroute at 17:53

192.168.1.2: guessing hop distance at 7

Completed Traceroute at 17:53, 0.17s elapsed

Initiating Parallel DNS resolution of 9 hosts. at 17:53

Completed Parallel DNS resolution of 9 hosts. at 17:53, 2.56s elapsed

SCRIPT ENGINE: Initiating script scanning.

Initiating SCRIPT ENGINE at 17:53

Completed SCRIPT ENGINE at 17:53, 1.25s elapsed

Host 192.168.1.2.track.net.br (192.168.1.2) appears to be up ... good.

Interesting ports on 192.168.1.2.track.net.br (192.168.1.2):

Not shown: 1699 closed ports

PORT   STATE   SERVICE   VERSION

25/tcp   filtered smtp

111/tcp   open   rpcbind

| rpcinfo:

| 100000 2   111/udp rpcbind

|_ 100000 2   111/tcp rpcbind

135/tcp   filtered msrpc

136/tcp filtered profile

137/tcp filtered netbios-ns

138/tcp filtered netbios-dgm

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

1533/tcp filtered virtual-places

1720/tcp filtered H.323/Q.931

6346/tcp filtered gnutella

8009/tcp open ajp13?

//Identifica o serviço ativo e qual a versão do mesmo

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_ HTML title: Apache Tomcat/5.5.23

12345/tcp filtered netbus

12346/tcp filtered netbus

31337/tcp filtered Elite

//identifica qual o SO instalado no Computador, mostrando uma lista com as principais possibilidades.

Aggressive OS guesses: Linux 2.6.11 - 2.6.19 (94%), Linux 2.6.21 (94%), Wireless broadband router (FON La Fonera, Linksys WAP54GL, or Netgear WGT634U) (OpenWrt, Linux 2.6.22) (94%), Linux 2.6.20 (Ubuntu, x86_64) (93%), Linux 2.6.22 (92%), Linux 2.6.20 (92%), Linux 2.6.9 - 2.6.15 (91%), Linux 2.6.18 (91%), Linux 2.6.23 (91%), Fortinet FortiGate-60 firewall, Linksys NSLU2 NAS device running Unslung 5.8 (Linux 2.4.22), Netgear SPH200D VoIP phone, Secure Computing SnapGear SG565 firewall (Linux 2.4.31-uc0), or Adaptec Snap Server 520 NAS device (91%)

//explica que não foi possível dizer exatamente qual o S.O.

No exact OS matches for host (test conditions non-ideal).

Uptime: 2.763 days (since Fri Aug 22 23:34:19 2008)

TCP Sequence Prediction: Difficulty=198 (Good luck!)

IP ID Sequence Generation: All zeros

//Indica quais os hops até o host alvo

TRACEROUTE (using port 111/tcp)

HOP RTT ADDRESS

1 0.00 192.168.2.1

2 0.00 acesso-250129.parttelecom.com.br (192.168.3.1)

3 15.00 rede60-17.parttelecom.com.br (192.168.4.1)

4 16.00 192.168.5.1

5 31.00 gw-caches.parttelecom.com.br (192.168.6.1)

6 31.00 BrT-F12-0-1-ldajc300.track.net.br (192.168.7.1)

7 31.00 BrTC-S2-0-3-1-ldajc300.track.net.br (192.168.8.1)

8   78.00 192.168.1.2.track.net.br (192.168.1.2)

Nmap done: 1 IP address (1 host up) scanned in 94.719 seconds

Raw packets sent: 1871 (85.716KB) | Rcvd: 1778 (82.594KB)

Observamos agora que o Nmap através de seu escaneamento e da sua base de dados sobre sistemas operacionais foi capaz de reconhecer com quase 100% de certeza que o sistema operacional presente no host era um sistema baseado em Linux, além de trazer informações sobre serviços ativos no host e qual sua versão. Se conseguimos essas informações com tamanha facilidade um atacante a obtém também.

Este segundo host também fora colocado atrás do nosso firewall, onde tentamos novamente, verificar qual seu Sistema Operacional com o comando:

nmap -T Aggressive -A -v -PN 192.168.1.2

Starting Nmap 4.65 (http://nmap.org) at 2008-08-25 18:42 Hora oficial do Brasil

Initiating Parallel DNS resolution of 1 host. at 18:42

Completed Parallel DNS resolution of 1 host. at 18:42, 0.06s elapsed

Initiating SYN Stealth Scan at 18:42

Scanning 192.168.1.2.brasiltelecom.net.br (192.168.1.2) [1715 ports]

SYN Stealth Scan Timing: About 16.36% done; ETC: 18:45 (0:02:34 remaining)

Completed SYN Stealth Scan at 18:45, 183.22s elapsed (1715 total ports)

Initiating Service scan at 18:45

Initiating OS detection (try #1) against 192.168.1.2.brasiltelecom.net.br (192.168.1.2)

Retrying OS detection (try #2) against 192.168.1.2.brasiltelecom.net.br (192.168.1.2)

SCRIPT ENGINE: Initiating script scanning.

Host 192.168.1.2.brasiltelecom.net.br (192.168.1.2) appears to be up ... good.

All 1715 scanned ports on 192.168.1.2.brasiltelecom.net.br (192.168.1.2) are filtered

Too many fingerprints match this host to give specific OS details

Read data files from: C:\Arquivos de programas\Nmap

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 189.813 seconds

Raw packets sent: 3478 (157.592KB) | Rcvd: 0 (0B)

Verificamos agora que o programa NMAP não é capaz de verificar qual o Sistema operacional presente no host em questão.

4.1.3. Firewalking

Para trabalharmos com o programa firewalk, que traz a funcionalidade da técnica de firewalking, utilizaremos a suíte Back Track 3 e a versão de firewalk presente no mesmo. Executamos um escaneamento, em um Servidor Linux Conectiva 10 através de um filtro de pacotes sem nenhum filtro ativado. A sintaxe do escaneamento foi a seguinte:

```
bt ~ # firewalk –n –p tcp –s80 –d80  192.168.5.10 192.168.1.2
```

onde:

- Comando –n → Utilizado para não resolver os endereços IP.
- Comando –p→ Utilizado para escolher o protocolo de escaneamento, TCP.
- Comando –s → Porta de origem, 80 (http).
- Comando –d → Porta de destino, 80 (http)

O primeiro endereço é do filtro de pacotes, e o segundo a métrica, que é o servidor Conectiva. Recebemos a seguinte resposta ao escaneamento:

```
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 80, destination port: 80
Hotfoot through 192.168.5.10 using 192.168.1.2 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.1.1]
 2 (TTL  2): expired [192.168.3.2]
 3 (TTL  3): expired [192.168.3.4]
 4 (TTL  4): expired [192.168.4.9]
 5 (TTL  5): expired [192.168.6.4]
 6 (TTL  6): expired [192.168.8.35]
 7 (TTL  7): expired [192.168.5.10]
Binding host reached.
Scan bound at 8 hops.
Scanning Phase:
port   1: A! open (port not listen) [192.168.1.2]
port   2: A! open (port not listen) [192.168.1.2]
port   3: A! open (port not listen) [192.168.1.2]
port   4: A! open (port not listen) [192.168.1.2]
port   5: A! open (port not listen) [192.168.1.2]
port   6: A! open (port not listen) [192.168.1.2]
port   7: A! open (port not listen) [192.168.1.2]
port   8: A! open (port not listen) [192.168.1.2]
port   9: A! open (port not listen) [192.168.1.2]
port  10: A! open (port not listen) [192.168.1.2]
...
port  41: A! open (port not listen) [192.168.1.2]
port  42: A! open (port not listen) [192.168.1.2]
port  43: A! open (port not listen) [192.168.1.2]
port  44: A! open (port not listen) [192.168.1.2]
port  45: A! open (port not listen) [192.168.1.2]
port  46: A! open (port not listen) [192.168.1.2]
```

```
port  47: A! open (port not listen) [192.168.1.2]
port  48: A! open (port not listen) [192.168.1.2]
port  49: A! open (port not listen) [192.168.1.2]
port  50: A! open (port not listen) [192.168.1.2]
port  51: A! open (port not listen) [192.168.1.2]
port  52: A! open (port not listen) [192.168.1.2]
port  53: A! open (port not listen) [192.168.1.2]
port  54: A! open (port not listen) [192.168.1.2]
port  55: A! open (port not listen) [192.168.1.2]
port  56: A! open (port not listen) [192.168.1.2]
...
//
port 111: A! open (port listen) [192.168.1.2]
port 112: A! open (port not listen) [192.168.1.2]
...
Scan completed successfully.
```

Verificamos que todos os pacotes passam pelo filtro e não são bloqueados em nenhum ponto chegando à métrica e mapeando todas as suas portas, dando o status, verificamos até uma porta ativa no host métrica, a porta 111 TCP.

Porém ao colocar o host atrás do firewall, mencionado nos estudos de caso anteriores, a resposta que recebemos é bem diferente.

```
bt ~ # firewalk -n -p tcp -s80 -d80 192.168.5.10 192.168.1.2
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 80, destination port: 80
Hotfoot through 192.168.5.10 using 192.168.1.2 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.1.1]
 2 (TTL  2): expired [192.168.3.2]
 3 (TTL  3): expired [192.168.3.4]
 4 (TTL  4): expired [192.168.4.9]
 5 (TTL  5): expired [192.168.6.4]
 6 (TTL  6): expired [192.168.8.35]
 7 (TTL  7): expired [192.168.5.10]
 8 (TTL  8): *no response*
 9 (TTL  9): unreach ICMP_UNREACH_HOST [192.168.5.10]
10 (TTL 10): unreach ICMP_UNREACH_HOST [192.168.5.10]
11 (TTL 11): *no response*
12 (TTL 12): unreach ICMP_UNREACH_HOST [192.168.5.10]
13 (TTL 13): unreach ICMP_UNREACH_HOST [192.168.5.10]
14 (TTL 14): unreach ICMP_UNREACH_HOST [192.168.5.10]
15 (TTL 15): *no response*
16 (TTL 16): unreach ICMP_UNREACH_HOST [192.168.5.10]
17 (TTL 17): unreach ICMP_UNREACH_HOST [192.168.5.10]
18 (TTL 18): unreach ICMP_UNREACH_HOST [192.168.5.10]
19 (TTL 19): *no response*
20 (TTL 20): unreach ICMP_UNREACH_HOST [192.168.5.10]
21 (TTL 21): unreach ICMP_UNREACH_HOST [192.168.5.10]
22 (TTL 22): unreach ICMP_UNREACH_HOST [192.168.5.10]
23 (TTL 23): *no response*
24 (TTL 24): unreach ICMP_UNREACH_HOST [192.168.5.10]
25 (TTL 25): unreach ICMP_UNREACH_HOST [192.168.5.10]
Scan aborted: hopcount exceeded.

Total packets sent:               25
```

Verificamos novamente que os pacotes não conseguem passar pelo firewall, devido a ação de nosso NAT, do firewall Stateful. Ou seja, se a conexão não tiver sido originada no interior da rede, não é possível, através desses comandos simples, passar pelo firewall.

Porém um atacante experiente e de posse de ferramentas de ataque mais sofisticadas, ou mesmo as ferramentas utilizadas neste estudo de caso, utilizando comandos mais elaborados pode conseguir acesso não autorizado à rede.

5. Conclusão

Firewalls e filtros de pacotes devem ser considerados equipamentos essenciais em uma rede de computadores, pois tem a capacidade de bloquear acesso indevido às redes em questão.

Porém, sem uma configuração adequada e sem conhecimento técnico dos administradores de rede sobre os riscos dos ataques externos (e, muitas vezes internos), a segurança dos dados, pode não ser satisfatória.

Os diferentes tipos de arranjos de hardware e software devem ser muito bem estudados e serem o mais adequados a rede, pois podem deixar brechas de segurança, que pessoas mal intencionadas podem utilizar para causar algum dano à instituição.

Os diferentes tipos de ataques existentes tornam-se obsoletos com o passar dos anos pela evolução que ocorre também nos métodos de defesa, mas, a engenhosidade e capacidade técnica de pessoas consideradas como Hackers é muito grande e estão sempre à procura de uma nova técnica de invasão que possa garantir-lhes acesso à rede.

As técnicas de firewalking já foram utilizadas em larga escala em ataques, que provavelmente deram muito trabalho a administradores dos mais variados locais do mundo. A solução mais fácil para este problema é bloquear mensagens ICMP TTL excedido através do firewall, afetando também mensagens válidas.

Outra possibilidade de defesa é a utilização de serviços de NAT (Network Address Translation), também conhecido como *masquerading*, onde se reescreve o endereço IP de origem de um pacote ao passar pelo firewall. Com este serviço pacotes da rede interna geram uma entrada no NAT para receberem uma resposta da rede externa. Pacotes originados de redes externas, ao chegarem ao router e não forem uma resposta a um pacote originado na rede interna, não terão entrada correspondente no NAT e será descartado, impossibilitando conexões indesejadas.

Com o adendo oferecido pelo NAT a vida das pessoas que atacam redes ficou um pouco mais difícil, porém essas pessoas são bastante determinadas e muito criativas.

Um novo estudo sobre técnicas de penetração pode ser elaborado aproveitando-se desta nova ferramenta de segurança.

Bibliografia

AKIN, Ofir. Network Scanning Techniques: Understanding How is Done. Disponível em: <http://www.sys-security.com/archive/papers/Network_Scanning_Techniques.pdf>. Acesso em: 02 maio 2008.

DANIELS, Thomas E.; SPAFFORD, Eugene H.. Subliminal Traceroute in TCP/IP. Disponível em: <http://csrc.nist.gov/nissc/2000/proceedings/papers/602.pdf>. Acesso em: 13 jan. 2008.

FIREWALL Disponível em: <http://pt.wikipedia.org/wiki/Firewall>. Acesso em: 12 abr. 2008.

GOLDSMITH, David; SCHIFFMAN, Michael. Firewalking: A Traceroute-Like Analysis of IP Packet Responses to Determine Gateway Access. Disponível em: <http://www.packetfactory.net/firewalk/firewalk-final.pdf>. Acesso em: 09 mar. 2008.

HOEFLER, Torsten. Remote Network Analysis. Disponível em: <http://www.ccc.de/congress/2004/fahrplan/files/54-verdeckte-netzwerkanalyse-paper.pdf>. Acesso em: 05 fev. 2008.

MODULO. Firewalls. Disponível em: <http://www.modulo.com.br/pdf/de7002pdf/firewalls.pdf>. Acesso em: 21 jan. 2008.

SCHIFFMAN, Mike D.. Building Open Source Network Security Tools: Components and Techniques. Indianapolis: John Wiley & Sons, 2003. 416 p.